Table of Contents

.01 **Purpose**. This Manual establishes policy, assigns responsibilities, and addresses high level standards and procedures for complying with the Bureau of Land Management (BLM) Information Technology (IT) Configuration Management (CM) process. CM is the process the BLM uses to manage, track, and document changes, to validate and test requirements, to ensure information is clear, concise, and valid, and to distribute and communicate changes to an IT asset throughout its life cycle.

.02 **Objectives**. The objectives of this Manual are to describe the CM process and its interrelationships to other activities, to convey CM's role in managing existing and future IT assets, and to furnish management officials and employees with a disciplined approach to documenting, managing, and tracking IT assets throughout their life cycle.

.03 **Authority**. The BLM CM process complies with the Clinger-Cohen Act "Section 5125 Agency Chief Information Officers, General Responsibilities," the Office of Management and Budget (OMB) Circular A-130 Appendix IV- Analysis of Key Sections, "2. Background", and the BLM IT Investment Management Process (IMP) Version 1.0.

.04 **Responsibility**. All personnel responsible for, or associated with use, acquisition, development, and maintenance of the BLM's hardware, software, telecommunications devices, system, user, and network documentation share responsibility for following the CM policy identified in this manual. The specific responsibilities assigned for CM are listed below:

A. **The Chief Information Officer** (CIO) is responsible for development, coordination, and overall management of IT investments and assets for BLM. The CIO also oversees BLM compliance with Federal and Departmental policies, guidelines, and regulations governing the management of these investments and assets.

B. **Assistant Directors** (ADs) are responsible for ensuring that CM process objectives are carried out within their areas of responsibility and ensuring that skilled Portfolio Managers and Project Managers are assigned to oversee and manage all IT systems and software under their jurisdiction.

C. **State and Center Directors** are responsible for ensuring that CM process objectives are carried out within their areas of responsibility and ensuring that a CM Manager is assigned for their IT installation.

D. **State/Center Chief Information Officers** are responsible for ensuring that CM process objectives are carried out within their areas of responsibility ensuring that IT investment decisions are integrated with program business needs.

E. **The Group Manager, Information Resource Management (IRM) Investment Management Group** (IMG) is responsible for ensuring that CM policy is understandable and complies with Federal, State, and Departmental laws and guidance.

F. **The Group Manager, System Coordination Office** (SCO) is responsible for ensuring that all investments under the direction of the National Information Technology Investment Board (NITIB) comply with the BLM's ITIMP.

G. **The Group Manager, Information Technology Services** is responsible for ensuring that CM process objectives are integrated into Washington Office business decisions and ensuring that a Configuration Manager is assigned for their IT installation.

H. **The Director, National Information Resources Management Center** (NIRMC) is responsible for providing operational support for distribution and testing of national applications, software, and hardware. The Director is also responsible for providing technical support for maintaining the NCM website, maintaining the national software repository, and providing assistance with test case and test plan development.

I. **The National Configuration Manager** is responsible for coordinating CM activities for the BLM including, but not limited to:

(1) Overseeing operation of the NCM process.

(2) Developing policy and procedures to implement an integrated BLM CM process.

(3) Coordinating policy development with State and Center Configuration Managers.

(4) Coordinating activities of the National Configuration Control Board (NCCB).

(5) Overseeing the baselines for national level applications, software, and hardware assets.

(6) Setting priorities for national applications and commercial-off-the-shelf (COTS) products through the National Configuration Test Environment (NCTE).

(7) Preparing briefings and educating senior level management and staff on CM policy, procedure, and processes.

(8) Assessing BLM CM training needs recommending a training curriculum to the CIO and the IMG manager.

J. **The NCM Administrator** is responsible for carrying out the day to day activities of the NCM staff including, but not limited to:

(1) Reviewing documents submitted to NCM for testing, scheduling, and validating assets prior to release to the NCM baselines;

(2) Managing the content of the NCM website;

(3) Facilitating the development of CM forms, evaluation tools, and Standard Operating Procedures (SOP) to implement a BLM CM process;

(4) Coordinating with State and Center Configuration Managers regarding changes to CM forms and NCM baseline management;

(5) Conducting CM assessments on National, State, Center, and project CM activities;

(6) Serving as backup to the National Configuration Manager.

K. **The NCM Specialist** is responsible for labeling, tracking, and managing all software and documents submitted to the NCM staff including, but not limited to:

(1) Preparing agendas for NCM meetings;

(2) Recording and publishing of the NCM meeting minutes;

(3) Providing initial screening of documents submitted to NCM;

(4) Maintaining the NCM document library;

(5) Coordinating with the NIRMC software distribution and project managers to ensure documentation and software are assigned an NCM tracking number.

L. **State and Center Configuration Managers** are responsible for coordinating CM activities for their State or Center including, but not limited to:

(1) Ensuring compliance with National, State, and Center CM policy; .

(2) Overseeing activities of the State or Center CM process;

(3) Providing guidance to State or Center CIOs and technical personnel on CM policy and procedures;

(4) Coordinating activities for State or Center Configuration Boards;

(5) Maintaining the State or Center hardware, software, and application baselines;

(6) Maintaining a local CM library;

(7) Coordinating with the NCM office on CM policy and procedures;

(8) Managing the content of State or Center CM websites ensuring that accurate and up-to-date information is posted;

(9) Providing activity reports to State or Center CIO, sponsors, owners, project managers, and the National Office or any other official designated by that CIO.

M. **State and Center Configuration Management Specialists** are responsible for labeling, tracking, and managing all software and documents submitted to the State or Center Configuration Manager including, but not limited to:

(1) Preparing agendas for CM related meetings;

(2) Recording and publishing of the State or Center CM meeting minutes;

(3) Providing initial screening of documents submitted to the Configuration Manager for review;

(4) Maintaining the State or Center document library and repository;

(5) Logging and assigning tracking numbers to documentation and software.

N. **Project Managers** are responsible for developing a CM plan as part of their responsibilities under the IMP for their projects and coordinating their project activities with National, State, or Center CM Specialists.

O. **Portfolio Managers** are responsible for managing the AD's IT investments and ensuring that CM procedures are applied during maintenance and upgrades of their software and hardware investments and that project implementation schedules are coordinated with other Portfolio Managers, the National Configuration Manager, and SCO staff.

P. **BLM Configuration Management Team** provides a forum to discuss State/Center and National issues affecting CM activities throughout the BLM and serves as a springboard for implementing CM policy and procedures. Each State and Center Configuration Manager is a member of the BLM Configuration Management Team (BCMT).

Q. **Configuration Boards** BLM will use Configuration Boards throughout all levels of the organization to manage its CM activities. At the national level, the board manages final release to the baseline for new investments under the direction of the CIO and the NITIB. They also oversee implementation planning and scheduling for those new assets. Meanwhile, State and Center level boards will function in a similar manner as the National Level board; however, they will also perform technical reviews of IT assets. Finally, the BLM will use project level boards to manage changes to project activities assuring that projects are documented, meet stated requirements, and conform to business needs.

S. **Information Technology Investments Board (ITIB)** approves acquisition of new investments at the State, Center, and National levels according to the criteria established in the BLM IMP.

T. **Technical Review Board (TRB)** ensures compliance with the BLM architecture and mediates disputes that may arise on architectural design issues.

U. **Other** Groups having responsibility for ensuring CM as defined within the BLM are the Application System Managers, System Owners, System Sponsors, General Support System Managers, User Representatives, System Administrators, and all other users. Their responsibilities will be discussed in detail in the BLM CM Handbook.

.05 **References**. The BLM CM Process complies with the Software Engineering Institute (SEI) Capability Maturity Model (CMM), Institute of Electrical and Electronic Engineers (IEEE) Software Engineering, Volume Two, Process Standards, 1999 Edition; BLM Information Technology Investment Management Process (ITIMP) Version 1.0, September 2001; General Accounting Office (GAO) Information Technology Investment Management (ITIM) Version 1, May 2000; BLM Configuration Management Guide Version 1.1 August 1996; and The Institute of Configuration Management, Configuration Management II (CMII) process.

.06 **Policy**. It is the policy of the BLM that all IT assets are monitored, tracked, documented, maintained, validated, controlled, and released under the BLM CM process. It is also the policy of BLM to use Configuration Boards to assist CIOs and ITIBs with managing changes to BLM's hardware, software, major applications, and telecommunication systems. Furthermore, it is the policy of the BLM that:

A. The National Configuration Manager oversees the BLM's CM process under the direction of the CIO. The National Configuration Manager shall implement and publish the change management process for National IT assets. All additions, changes, or deletions to the National baselines (hardware, software, or documentation) will be accomplished through the change management process. (BLM CM Handbook, Section 2.5)

B. The State or Center Configuration Managers oversee their State or Center CM process under the direction of the appropriate CIO. Each State and Center Configuration Manager will implement and publish the change management process for IT assets under their jurisdiction. All additions, changes, or deletions to the State or Center baselines (hardware, software, or documentation) will be accomplished through the change management process. (BLM CM Handbook, Section 2.5)

C. The National, State, or Center change management process will include what items are placed under formal management, who must review and the corresponding sign-off authority before it can be released to the CM baselines. (BLM CM Handbook, Section 2.5.6)

D. Configuration Boards shall be an integral part of the change management process. The National, State, and Center level boards will provide additional oversight on newly acquired software and hardware assets. Project Managers shall use Project level boards to manage changes in newly acquired national software application development projects. (BLM CM Handbook, Section 2.4.1)

E. All configuration settings for software and hardware shall be documented, maintained, distributed, and managed in accordance with the CM process. (BLM CM Handbook, Section 2.5.6)

F. All documentation associated with release of an IT asset to the CM baseline with its correlating software or application shall be assigned a unique name and number by the appropriate BLM CM Specialist. Project managers shall consult with their BLM CM Specialist regarding naming and numbering of their project level documentation and software. (BLM CM Handbook, Section 2.5.8)

G. The National, State, and Center Configuration Managers shall maintain an accurate up-to-date baseline listing of applications, hardware, and software. (BLM CM Handbook, Section 2.5.9)

H. All documentation related to release of an IT asset to the National, State, or Center baseline shall be kept in secure storage under formal control of the appropriate BLM CM Specialist. (BLM CM Handbook, Section 2.5.10)

I. All distributions of National IT assets shall be coordinated through State and Center Configuration Managers. State and Center Configuration Managers shall confirm receipt of IT assets to the NCM Office. Furthermore, all distributions of State and Center IT assets shall be coordinated through the State and Center Configuration Managers. (BLM CM Handbook, Section 2.1.2)

J. Each Configuration Manager shall maintain a copy of the IEEE software process development standard. All project managers, system owners, and system sponsors must comply with this standard. (BLM CM Handbook, Section 2.8)

K. All National, State, and Center software IT assets shall be tested, coordinated, and validated using cross functional or integrated project teams. (BLM CM Handbook, Section 2.2.9)

L. The National Configuration Manager, State and Center Configuration Managers, State and Center CIOs, and other designated personnel within the ITIMP shall ensure that non-IT and IT professionals follow the CM process. (BLM CM Handbook, Sections 2.2.7 and 2.2.8)

M. Sponsors shall identify system owners, project managers, and user representatives according to the ITIMP to make decisions about an IT asset throughout its life cycle. (BLM CM Handbook, Section 2.6)

N. Employees shall consult with their State or Center Configuration Manager and review the IT Clearinghouse before presenting a proposal to acquire an IT asset for National, State, or Center usage to the appropriate National, State, or Center ITIB. (BLM CM Handbook, Section 2.6)

.061 **Scope**. The policy contained in this document applies to all BLM resources at all levels. This policy is mandatory for all organizational units, employees, contractors, and others having access to and/or using the IT resources of the BLM. This Manual will be applied to all existing and future IT investments. It will also be applied to all internal service level agreements between organizational units, interagency agreements, and contracts made between BLM and other public and private organizations.

.062 **Background**. CM is one of the "key process areas" in improving the BLM's IMP as referenced in the GAO's AMID-10.1.23 and it is essential for bringing the needed accountability to the BLM's IT assets and investments. Although CM is commonly associated with managing software application development activities, it is a process that allows us to manage, track, validate, document, monitor, release, and control changes to all our software and hardware investments. It is also the process that allows us to evaluate and implement changes and assure traceability and compatibility throughout an investment's life cycle. Finally, the CM process focuses on assuring availability, integrity, accountability, interoperability, and documentation of all IT investments and assets.

.07 **File and Records Maintenance**. CM will maintain its records in compliance with the BLM Records Management policy and procedures. The CM process focuses on ensuring that only authorized personnel have access to software media, electronic and paper records under formal CM management and through establishing a clear chain of control minimizes the risk of unauthorized alteration or erasure of documents under formal CM management.

.08 **Coordination Requirements**. CM policy and procedures will be coordinated and disseminated through State or Center Configuration Managers. Configuration Managers will assure that CIOs, IT Security, Records, Data, System Administrators, Help Desk Personnel, Project Managers, and User Representatives are kept informed of CM related activities and that personnel identified in the Change Management Process are included in all reviews. State and Center Configuration Managers will produce status reports of CM activities to share with other Configuration Managers on the monthly BLM Configuration Managers conference call. Project Managers will coordinate CM documents, software requests, and testing through the appropriate BLM CM Specialist.

.09 **Relationships With Other IT Activities**. This section describes the roles of other activities that interface with particular aspects of CM. Those activities are as follows: Data Administration, Freedom of Information Act (FOIA), IT Security, Life Cycle Management (LCM), Telecommunications, Architecture, and Records Administration. The National Configuration Manager will provide the interface at the Bureau level and will work very closely with the above activities. The following paragraphs describe the responsibilities of each activity.

A. **Data Administration** objectives are to establish policy, procedures, and standards that guide the BLM's efforts in effective management of information. The focus is on preserving the integrity and security of data collected, used, and shared within the BLM. Data Administration includes the concepts of data quality, data privacy, data security, and database integrity.

B. **Freedom of Information Act** (FOIA) objectives are to provide any person the right to access federal records, except for records (or portions thereof) that are protected from disclosure by one of nine exemptions. This statue also requires specific information, such as agency rules, regulations, and final decisions are made available as public records. The FOIA is a disclosure statute but recognizes that the Government is responsible for safeguarding the confidentiality of sensitive personal, commercial, and governmental (proprietary/confidential) information.

C. **IT Security** is responsible for the functional components of the IT Security Program. The program includes managing all aspects of information security which include administrative, personnel, technical, physical, and telecommunications security.

D. **Life Cycle Management** provides a uniform methodology to developing applications and implementing an IT system. LCM is the process of managing a system from cradle to grave. It represents a structured approach to solving information management needs. LCM covers a broad range of activities, from the identification of a problem or need, to the replacement and archiving of the system.

E. **BLM Telecommunications Activities** provide for the management (planning, operation, and maintenance) of the BLM's telecommunication systems, networks, equipment and services, and defines responsibilities. The program provides all BLM telecommunications support in accordance with current statutes, standards, rules, and regulations governing the planning for, acquisition, operation and maintenance, and disposal of such capabilities.

F. **Records Administration** objectives are to establish policy, procedures, and standards for records maintained in electronic and manual forms throughout the life cycles. This includes creation, maintenance, use, disclosure, and disposition of information. These policy and procedures must be documented and disseminated through the BLM Directives System. Proper administration of records/data/information must be exercised to ensure that the legality, integrity, access, sharing and exchange, and security standards are met. This also includes managing the inventory and disposition of electronic and manual records.

G. **Bureau Enterprise Architecture** objectives are to provide a management framework describing "what" needs to happen rather than "how" it should happen. It applies business rules and processes required to operate the organization that are independent of any specific organizational structure, technology, existing systems, hardware, and software needed in basic operation of the BLM.

Glossary of Terms

Baseline. A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development or acquisition, and that can be changed only through formal CM process change control procedures. (IEEE-STD610)

Change Request. Request arising through changes in the business or issues in the project. Change requests should be logged, assessed, and agreed on before a change to the project can be made. Changes may affect the scope, quality, time, and/or cost of the project and/or other planned aspects of the project.

Commercial-off-the-shelf (COTS) An item produced and placed in stock by a distributor before receiving orders or contracts for its sale. (Excerpt from FAR 46.101) is a product developed to perform specific functions without changes.

Configuration Library. A repository that is used for the safekeeping and storage of Configuration Management (software, hardware, and documentation) references materials.

Hardware. Physical equipment as opposed to programs, procedures, rules, and associated documentation. A physical item distinguished by the capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts.

Release. A term used generally to identify software and documentation that have gone through the CM process and approved for use throughout the BLM.

Requirements. A term used to denote explicit functions and products that are needed to perform or implement an IT investment or asset.

Software. A combination of associated computer instructions and computer data definitions required to enable computer hardware to perform computational or control functions.

Validate. A term used to denote checking for compliance with prescribed set of standards to verify the accuracy of the information.

Appendix - Acronyms and Abbreviations

AD	Assistant Director
BCMT	BLM Configuration Management Team
BLM	Bureau of Land Management
CIO	Chief Information Officer
CM	Configuration Management
CMM	Capability Maturity Model
COTS	Commercial-off-the-Shelf
FOIA	Freedom of Information Act
GAO	General Accounting Office
IEEE	Institute of Electrical and Electronic Engineers
IMG	Investment Management Group
IMP	Investment Management Process
IRM	Information Resources Management
IT	Information Technology
ITIB	Information Technology Investment Board
ITIM	Information Technology Investment Management
ITIMP	Information Technology Investment Management Process
LCM	Life Cycle Management
NCCB	National Configuration Control Board
NCM	National Configuration Management
NCTE	National Configuration Test Environment
NIRMC	National Information Resource Management Center
NITIB	National Information Technology Investment Board
OMB	Office of Management and Budget
SCO	System Coordination Office
SEI	Software Engineering Institute
SOP	Standard Operating Procedure
TRB	Technical Review Board